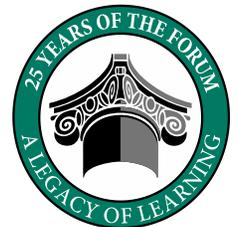


Card Fraud Trends and Updates



Presented by
Matthew Cissne
Bank of America
Merrill Lynch



FORUM2013

Agenda

- **Welcome**
- **Introduction**
- **Card Fraud Introduction**
- **Data Breaches**
- **Phishing and Malware**
- **Card Fraud Mitigation**
- **Best Practices**
- **Employee Abuse/Misuse**
- **Questions and Answers**

Threat Landscape

February 16, 2013

Facebook hacked, social media company says

By Tim Reid

"Last month, Facebook security discovered that our systems had been targeted in a sophisticated attack," the company said in a blog post. "The attack occurred when a handful of employees visited a mobile developer website that was compromised."

The social network, which says it has more than one billion active users worldwide, added: "Facebook was not alone in this attack. It is clear that others were attacked and infiltrated recently as well."

September 19, 2012

Chase joins Bank of America in possible Islamic attack outage

By Rik Myslewski

"We're experiencing intermittent issues with Chase.com," a JPMorgan Chase spokesman told MSN Money. "We apologize for any inconvenience and are working to restore full connectivity."

Bank of America suffered similar problems yesterday. A bank spokesman told Reuters at the time that "We are working to ensure full availability," and assuring customers that "We continuously take proactive measures to secure our systems."

By Cyber Attack



The attacks mark the highest-profile cyber attacks to date on businesses running Mac computers.

Hackers have traditionally focused on attacking machines running the Windows operating system, though they have gradually turned their attention to Apple products over the past couple of years.

"This is the first really big attack on Macs," the source told Reuters.

"Apple has more on its hands than the attack on itself."

Cyber-security attacks have been on the rise.

In last week's State of the Union address, US President Barack Obama issued an executive order seeking better protection of the country's critical infrastructure from cyber attacks.

December 27, 2012

DDoS: Citi Takes Post-Holiday Hit

By Tracy Kitten

DDoS: Citi Takes Post-Holiday Hit
Hacktivists Announce Plans for Year-End Bank Attacks
By Tracy Kitten, December 27, 2012.

After hacktivists announced in a Christmas Day Pastebin post plans for a third week of bank attacks, Citigroup reported site interruptions Dec. 26 that struck during the late afternoon.

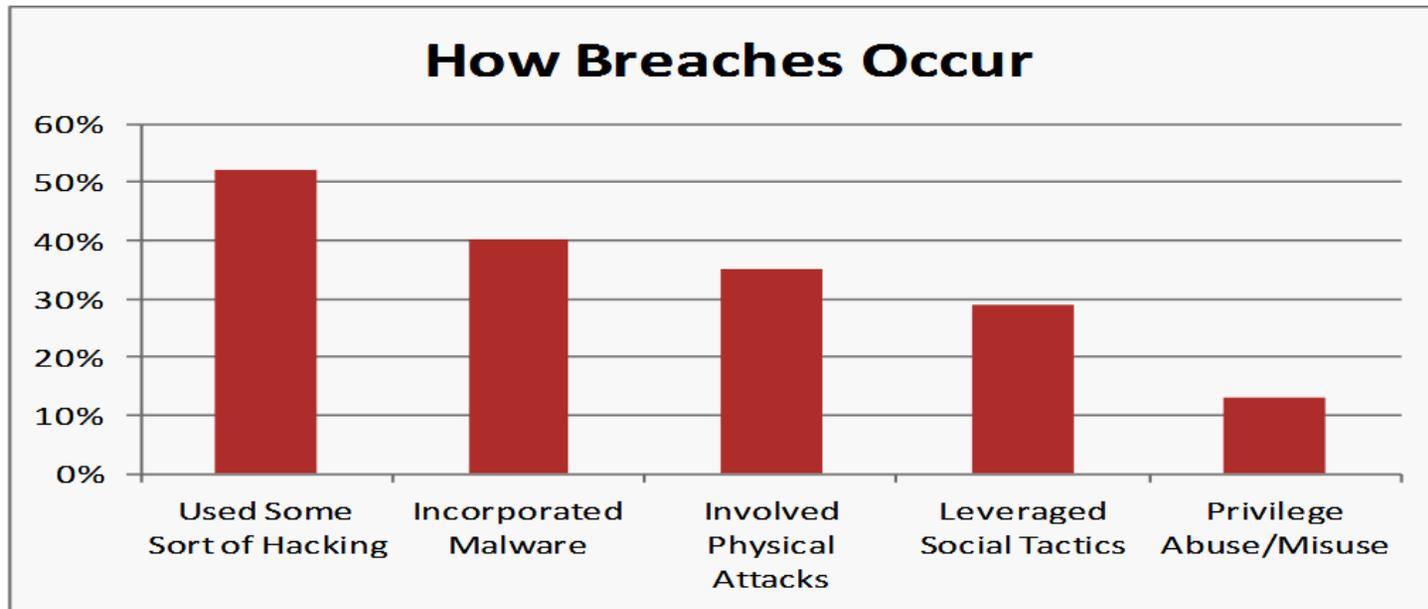
Citi spokesman Andrew Brent did not attribute the online-banking access issues to high volumes of traffic, as is typical in a distributed-denial-of-service attack, saying that the bank does not disclose details about IT infrastructure issues.

Fraud – The theft of card information by fraudsters

- Account takeover (information change)
- Counterfeit cards
- Lost/Stolen cards
- Card Not Present
- Skimming
- Database Hacking
- Franchise Software Hacking
- Phishing

Abuse – Intentionally or unintentionally violating policies and procedures for personal gain

Misuse – Intentionally or unintentionally violating policies and procedures for work related gain



Data: Verizon 2013 Data Breach Investigations Report

Definitions:

- **Hacking** – Act of breaking into computer systems to access or harm data without authorization
- **Malware** – Slang for malicious software which may include emails including links that open to web pages or PDF, pop up windows, free software, which are all ploys used to exploit data; may include key logging virus or spyware that records all keyboard activity
- **Physical Attacks** – Encompasses internal employee actions that require physical proximity to servers or PCs to obtain data or tapping with point-of-sale terminals
- **Social Attacks** – Tactics that employ deception, manipulation, intimidation to exploit the human element can be with monetary rewards but most common data obtained is sold underground as hot commodities
- **Privilege Misuse** – Internal data access that may be intentional or unintentional including embezzlement, skimming, and system abuse

Ongoing Servicing Mitigation

- Immediately monitor all transaction activity within fraud to prevent high risk activity
- Notify cardholders and clients that require card to be replaced
- As appropriate, conduct exception processing to accommodate cardholder special requests, including overnight plastics to expedite receipt of cards

Cardholder Notification

- Recent change in certain state laws mandate that entity must notify cardholders of data breach
- May result in client/cardholders being informed before bank targets accounts for replacement
- Notification may come from a 3rd party vendor or via media notification (i.e. press release or internet)

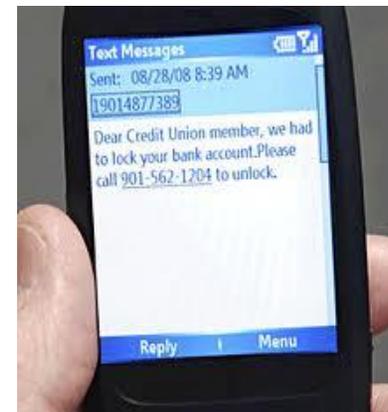
External Data Compromise Fraudsters are patient in leveraging data obtained

Action for Cardholders

- If concerned, please contact your Bank of America Merrill Lynch representative or Fraud department at (866) 500-8262 or the telephone number on the back of your card

Fraudsters attack weakest point in the transaction

- **Phishing & SMishing:** Infected files/malicious links sent through email or SMS message
- **Drive by Downloads:** Clicking on a document, ad, or video, posted on legitimate website initiates malware download
- Use of infected flash drive
- Credential theft and/or HTML injection
- **Transaction Takeover**
 - Trojan is silently activated
 - Trojan stores or actively relays user's activities without the user knowing
 - Trojans are coded to watch for one or more online banks



Phishing emails used to harvest data, infect devices

Phishing and spoofing emails look like official Bank of America Merrill Lynch emails and try to trick you into visiting a fake website and providing your personal account information. E-mails will often contain links that can result in Malware infected devices.

-----Original Message-----

From: Bank of America Alert

[mailto:onlinebanking@alert.fraud.edu]

Sent: Sunday, May 09, 2010 4:55 PM

To: Cissne, Matt

Subject: Bank of America Alert: Irregular Credit Card Activity

Dear Customer:

We detected irregular activity on your Bank of America credit card on 09/May/2010.

To safeguard your account, we've classified it as dormant.

What does this mean for you?

You will not be able to use your credit card, until it has been reactivated. The process for reactivation is simple:

- 1. Download the activation form.**
- 2. Enter basic security information**

Don't forget - your credit card can be used anywhere VISA® or MasterCard® is accepted so once you've reactivated your account, you're free to spending money.

If you do not reactivate your account, your account will remain dormant.

Yours sincerely,

Ways to identify Phishing from Bank of America Merrill Lynch contacts

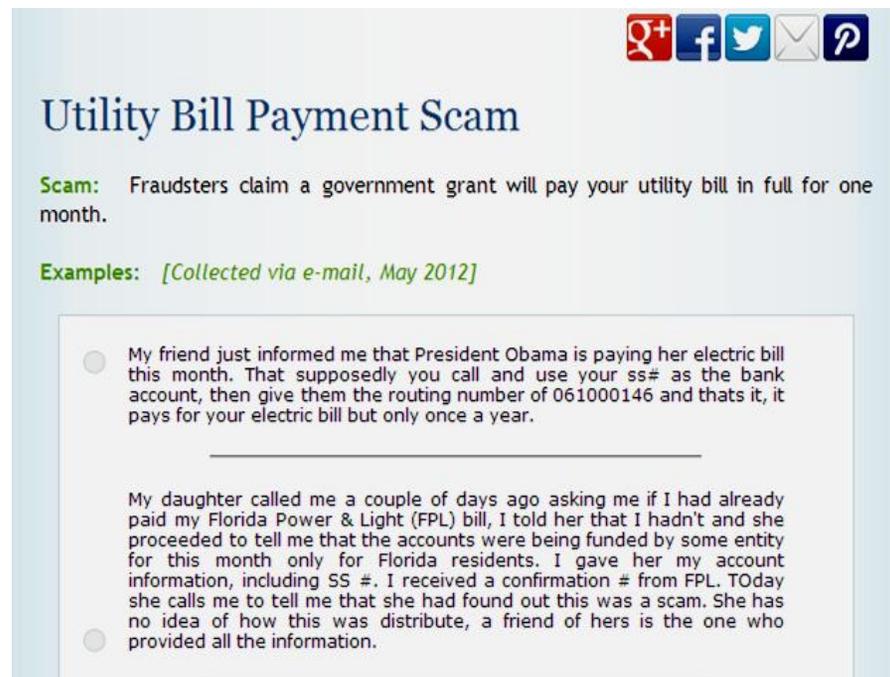
- Bank of America Merrill Lynch will not ask client or cardholder to provide account number and/or personal information via an email
- Most fraudulent communications convey a sense of urgency by threatening discontinuing service or declining authorizations
- Many fraudulent emails contain misspellings, incorrect grammar, and poor punctuation
- Links within the email may appear valid, but deliver you to a fraudulent site
- Phishing emails often use generic salutations like "Dear Customer," or "Dear account holder" instead of your name
- All legitimate Bank of America Merrill Lynch emails will include telephone number to contact office

Actions for Clients

- Do not provide sensitive data via e-mail or unsolicited web page
- Forward any emails if received to abuse@bankofamerica.com
- If concerned, please contact your account manager, the Fraud department or the telephone number on the back of your card

Federal Government to pay your utility bills

- Staged introductions into different markets
- Social Media (primary) and Email (secondary) distributed
- Instructed customers to call a number to receive their government grant
- Customers provided Utility information, SSN, Bank Account information
- Fraudster provided Account Number, RT/ABA, and grant confirmation number to be used for government grant
- Provided customer with bill pay VRU at Utility Company
- Customer called bill pay phone number and entered information
- Received notice from Utility Company that payment was returned and account was overdue



Utility Bill Payment Scam

Scam: Fraudsters claim a government grant will pay your utility bill in full for one month.

Examples: *[Collected via e-mail, May 2012]*

My friend just informed me that President Obama is paying her electric bill this month. That supposedly you call and use your ss# as the bank account, then give them the routing number of 061000146 and thats it, it pays for your electric bill but only once a year.

My daughter called me a couple of days ago asking me if I had already paid my Florida Power & Light (FPL) bill, I told her that I hadn't and she proceeded to tell me that the accounts were being funded by some entity for this month only for Florida residents. I gave her my account information, including SS #. I received a confirmation # from FPL. Today she calls me to tell me that she had found out this was a scam. She has no idea of how this was distribute, a friend of hers is the one who provided all the information.

Snopes.com

Are you prepared to identify and manage events like these?

Detection:

- Social Media Monitoring
- Bill Pay account changes – online and VRU
- Bill Pay VRU increased activity
- Contact Center inquiries
- Return payment activity monitoring

Impact to Consumers:

- Victim of Identity Theft
- Credit Monitoring and bank information changes
- Financial loss, inability to pay current bills

Impact to Company:

- Potential Impact to cash flow
- High ACH return rates – implications to future direct debit programs
- Media visibility and brand impact
 - Were you proactive or reactive?
 - What support did you offer impacted customers?

Sample Social Media Dashboard (socialmediaexaminer.com)



Authorizations that Fraud Needs to Validate

- Outbound Call to Primary Contact listed on account to verify activity
- If no answer, Outbound Call to Secondary contact listed on the account
- If no answer at either telephone numbers or outside of calling hours, email sent to primary contact

Posted Fraud Charges that Require Credit

- Following fraud confirmation, the account will be closed and each transaction transferred to new account
- All transactions will appear on the new account number billing statement or your reporting tool
- Fraud Claims may send a fraud statement to the PA or cardholder via email, fax or regular mail
- PA or cardholder may be asked to complete Fraud Affidavit to comply with VISA and MasterCard regulations
- Credits for individual fraud transactions will appear on new account for balance reconciliation

Actions for Clients/Cardholders

- Fraud department 866-500-8262 or collect 509-353-6656 is available 24/7 to assist with questions or verification

Industry Recognition

- Ranked #1 for Fraud Prevention by Javelin Strategy and Research for last 8 years
- Consistently achieve < 3 bps of fraud compared to Transaction Volume for last 5 years – half of peer competitors
- Leader in Industry Forums regarding Fraud Mitigation strategies

Internal 2012 Results

- Balance Client Experience and fraud mitigation in every decision
- Achieved 90+% Satisfaction Rating from our Clients in Fraud Survey in 2012
- Fraud strategies impact less than .2% of all card transactions
- Continue to invest in industry leading tools to mitigate fraud and reduce impact to our clients

Provide custom fraud solutions to assist clients as needed

Card Industry Best Practices

Client Controls

Create guidelines for card issuance and handling

- Determine who should be eligible to apply for a card
- Determine approval levels required
- Segregate duties of ordering and receiving of cards

Create internal procedures

- Requirements for obtaining a card
- Administrative / Management
- Usage / Purchasing
- Accounts Payable/Accounting
- Reconciliation
- Audit

Create policies or business rules

- Business versus Personal Use
- Cash access
- Card sharing
- Ghost cards
- Roles and responsibilities
- Training
- Audit exceptions

Program Administrators

- Ensure cardholder statement reconciliation is performed in a timely manner
- Monitor declined authorizations for signs of merchant and/or employee abuse
- Manage credit limits based on individual cardholder spending needs
- Consider MCC (Merchant Category Codes) restrictions and \$ thresholds to prevent internal and fraud abuse
- Complete internal audits of transaction monitoring at MCC and cardholder levels
- Provide Bank of America Merrill Lynch after hours contacts including telephone numbers and emails for prompt contact to detect and prevent fraud
- Partner with fraud team future for current authorization needs to improve control with least amount of cardholder impact

Best Practices for Audit Metrics

Audit high-risk transactions monthly

- Cardholders with the highest number of transactions
- Cardholders with the highest dollar amount spent
- Employees with multiple disputes
- Purchases charged to clients
- Increase frequency for those cardholders with exceptions Audit representative samples - within 60-90 days new account

Vendors

- Number of vendors utilized
- Transactions per vendor
- Transactions between a cardholder and same vendor

Reconciliation

- # and \$ of transactions between a cardholder and same vendor
- Review items not submitted or duplicate expense reports for same transaction
- Accountable property transactions logged
- Transactions from approved suppliers
- Transactions reconciled using default funding
- Split purchase occurrences to avoid dollar thresholds

Requirements for Service

- Free Misuse/Abuse Insurance service for clients with use of commercial card program
- Associate involved must be terminated to qualify for insurance coverage
- Association covers 75 days prior to termination and 14 days after
- \$100,000 per cardholder
- No exclusion on transaction types

Posted Abuse Charges that Require Credit

- Notify Bank of America Merrill Lynch of account closure or complete cancelation of account ASAP to protect interests
- Contact Fraud team to determine next steps with possible recovery efforts
- Association requires form and supporting documents to be provided to file claim
 - Verification of associate dismissal
 - Itemization of the charges that are involved in case
 - Standard form to be completed
- Bank of America Merrill Lynch files paperwork with the association on your behalf
- Bank of America sends demand letter to cardholder involved as component to Visa requirements
- Subsequent credit will be applied to credit card account
- Expect 30–60 days for resolution

Everyone Has a Role/Responsibility in Fraud Prevention

- Industry
- Organizations
- Financial Institutions
- Individuals
- Law Enforcement
- Media
- Other Interested Parties

Be diligent in all transactions and vendor interactions

Contact your Bank of America Merrill Lynch representative to assist with concerns/questions

Appendix

Bank of Am
Merrill Lyn

Vendor Services and Mobile Security

Vendor Services

- Perform site review and engage all resources to assist in decision making
- Review internal needs and allow vendor access only to required data and limit log-ins to limit potential breaches
- Ask and understand the vendor's loss recovery processes and service level agreements currently in place
- Do your homework – check references, awards, or company standards regarding product and data security processes and procedures to ensure a balanced risk/reward decision

Mobile Devices

- Choose devices carefully – select device that provides encryption and authentication capabilities
- Use Intrusion Prevention software
- Control and limit third party applications downloads
- Limit Bluetooth capabilities – switch to hidden or turn off broadcast when not in use
- Avoid using an automatic login features that save usernames and passwords for online banking

Industry Best Practices for Data Access

- Encrypt sensitive information, laptops, and removable storage devices
- Control how users access information
- Be careful that the devices of departing workers are securely wiped
- Install a dedicated, actively-managed Firewall
- Limit network administrative rights for users
- Make certain computers are running all current operating system patches and updates to prevent unauthorized access
- Install and maintain real time anti-virus, anti-malware and spyware software applications



Identity Theft – Definition and Contacts

Identity theft occurs when someone uses your personal information including name and social security number without your permission to commit fraud or other crimes.

- Federal Trade Commission estimates 9 million identities are stolen each year
- Can impact ability to obtain housing, employment and bank accounts

Ways to identify ID Theft Identification

- Obtain annual credit bureau report to check for any unknown activity:
<https://www.annualcreditreport.com/cra/index.jsp>
- Negative changes in credit lines, interest rates or other unexpected changes to established accounts

Credit Bureau Contacts if you suspect ID Theft:

TransUnion: 1-800-680-7289; www.transunion.com Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92834-6790

Equifax: 1-800-525-6285; www.equifax.com P.O. Box 740241, Atlanta, GA 30374-0241

Experian: 1-888-EXPERIAN (397-3742); www.experian.com P.O. Box 9554, Allen, TX 75013

Identity Theft Prevention: Best Practices

- Avoid providing your Social Security Number unless you have initiated the request and confirmed the business and person's identity
- Do not list Social Security Number on checks or carry ID card in your wallet
- Monitor bank statements, credit card statements, and check your credit report
- Shred personal documents
- Never save credentials or personal information on unknown or community computers
- Guard your laptop, cell phone and other technology against theft
- Don't leave important mail sitting in physical mailbox
- When possible, request "Signature Required" when receiving sensitive mail via courier such as FedEx or UPS
- Be cautious when using the ATM by covering your PIN and taking your receipt, or don't request a receipt

Disclaimer

“Bank of America Merrill Lynch” is the marketing name for the global banking and global markets businesses of Bank of America Corporation. Lending, derivatives, and other commercial banking activities are performed globally by banking affiliates of Bank of America Corporation, including Bank of America, N.A., member FDIC. Securities, strategic advisory, and other investment banking activities are performed globally by investment banking affiliates of Bank of America Corporation (“Investment Banking Affiliates”), including, in the United States, Merrill Lynch, Pierce, Fenner & Smith Incorporated and Merrill Lynch Professional Clearing Corp., which are both registered broker dealers and members of FINRA and SIPC, and, in other jurisdictions, by locally registered entities.

Investment products offered by Investment Banking Affiliates: Are Not FDIC Insured * May Lose Value * Are Not Bank Guaranteed.

These materials have been prepared by one or more subsidiaries of Bank of America Corporation for the client or potential client to whom such materials are directly addressed and delivered (the “Company”) in connection with an actual or potential mandate or engagement and may not be used or relied upon for any purpose other than as specifically contemplated by a written agreement with us. These materials are based on information provided by or on behalf of the Company and/or other potential transaction participants, from public sources or otherwise reviewed by us. We assume no responsibility for independent investigation or verification of such information (including, without limitation, data from third party suppliers) and have relied on such information being complete and accurate in all material respects. To the extent such information includes estimates and forecasts of future financial performance prepared by or reviewed with the managements of the Company and/or other potential transaction participants or obtained from public sources, we have assumed that such estimates and forecasts have been reasonably prepared on bases reflecting the best currently available estimates and judgments of such managements (or, with respect to estimates and forecasts obtained from public sources, represent reasonable estimates). No representation or warranty, express or implied, is made as to the accuracy or completeness of such information and nothing contained herein is, or shall be relied upon as, a representation, whether as to the past, the present or the future. These materials were designed for use by specific persons familiar with the business and affairs of the Company and are being furnished and should be considered only in connection with other information, oral or written, being provided by us in connection herewith. These materials are not intended to provide the sole basis for evaluating, and should not be considered a recommendation with respect to, any transaction or other matter. These materials do not constitute an offer or solicitation to sell or purchase any securities and are not a commitment by Bank of America Corporation or any of its affiliates to provide or arrange any financing for any transaction or to purchase any security in connection therewith. These materials are for discussion purposes only and are subject to our review and assessment from a legal, compliance, accounting policy and risk perspective, as appropriate, following our discussion with the Company. We assume no obligation to update or otherwise revise these materials. These materials have not been prepared with a view toward public disclosure under applicable securities laws or otherwise, are intended for the benefit and use of the Company, and may not be reproduced, disseminated, quoted or referred to, in whole or in part, without our prior written consent. These materials may not reflect information known to other professionals in other business areas of Bank of America Corporation and its affiliates.

Bank of America Corporation and its affiliates (collectively, the “BAC Group”) comprise a full service securities firm and commercial bank engaged in securities, commodities and derivatives trading, foreign exchange and other brokerage activities, and principal investing as well as providing investment, corporate and private banking, asset and investment management, financing and strategic advisory services and other commercial services and products to a wide range of corporations, governments and individuals, domestically and offshore, from which conflicting interests or duties, or a perception thereof, may arise. In the ordinary course of these activities, parts of the BAC Group at any time may invest on a principal basis or manage funds that invest, make or hold long or short positions, finance positions or trade or otherwise effect transactions, for their own accounts or the accounts of customers, in debt, equity or other securities or financial instruments (including derivatives, bank loans or other obligations) of the Company, potential counterparties or any other company that may be involved in a transaction. Products and services that may be referenced in the accompanying materials may be provided through one or more affiliates of Bank of America Corporation. We have adopted policies and guidelines designed to preserve the independence of our research analysts. The BAC Group prohibits employees from, directly or indirectly, offering a favorable research rating or specific price target, or offering to change a rating or price target to a subject company as consideration or inducement for the receipt of business or for compensation and the BAC Group prohibits research analysts from being directly compensated for involvement in investment banking transactions. We are required to obtain, verify and record certain information that identifies the Company, which information includes the name and address of the Company and other information that will allow us to identify the Company in accordance, as applicable, with the USA Patriot Act (Title III of Pub. L. 107-56 (signed into law October 26, 2001)) and such other laws, rules and regulations as applicable within and outside the United States.

We do not provide legal, compliance, tax or accounting advice. Accordingly, any statements contained herein as to tax matters were neither written nor intended by us to be used and cannot be used by any taxpayer for the purpose of avoiding tax penalties that may be imposed on such taxpayer. If any person uses or refers to any such tax statement in promoting, marketing or recommending a partnership or other entity, investment plan or arrangement to any taxpayer, then the statement expressed herein is being delivered to support the promotion or marketing of the transaction or matter addressed and the recipient should seek advice based on its particular circumstances from an independent tax advisor. Notwithstanding anything that may appear herein or in other materials to the contrary, the Company shall be permitted to disclose the tax treatment and tax structure of a transaction (including any materials, opinions or analyses relating to such tax treatment or tax structure, but without disclosure of identifying information or, except to the extent relating to such tax structure or tax treatment, any nonpublic commercial or financial information) on and after the earliest to occur of the date of (i) public announcement of discussions relating to such transaction, (ii) public announcement of such transaction or (iii) execution of a definitive agreement (with or without conditions) to enter into such transaction; provided, however, that if such transaction is not consummated for any reason, the provisions of this sentence shall cease to apply. Copyright 2013 Bank of America Corporation.